



Implementing DHCP for IPv6

This module describes how to configure Dynamic Host Configuration Protocol (DHCP) for IPv6.

- [DHCPv6 Prefix Delegation, on page 1](#)
- [How to Implement DHCP for IPv6, on page 6](#)

DHCPv6 Prefix Delegation

The IPv6 Access Services—DHCPv6 Prefix Delegation feature can be used to manage link, subnet, and site addressing changes. Dynamic Host Configuration Protocol for IPv6 (DHCPv6) can be used in environments to deliver stateful and stateless information, which are defined as follows:

- Stateful prefix delegation—Address assignment is centrally managed and clients must obtain configuration information such as address autoconfiguration and neighbor discovery that is not available through protocols.
- Stateless prefix delegation—Stateless configuration parameters do not require a server to maintain any dynamic state for individual clients, such as Domain Name System (DNS) server addresses and domain search list options.

Extensions to DHCPv6 also enable prefix delegation, through which an ISP can automate the process of assigning prefixes to a customer for use within the customer's network. The prefix delegation occurs between a provider edge (PE) device and customer premises equipment (CPE) using the DHCPv6 prefix delegation option. Once the ISP has delegated prefixes to a customer, the customer may further subnet and assign prefixes to the links in the customer's network.

Configuring Nodes Without Prefix Delegation

Stateless DHCPv6 allows DHCPv6 to be used for configuring a node with parameters that do not require a server to maintain any dynamic state for the node. The use of stateless DHCP is controlled by router advertisement (RA) messages multicasted by routers. The Cisco IOS XE DHCPv6 client will invoke stateless DHCPv6 when it receives an RA. The Cisco IOS XE DHCPv6 server will respond to a stateless DHCPv6 request with configuration parameters, such as the DNS servers and domain search list options.

Client and Server Identification

Each DHCPv6 client and server is identified by a DHCP unique identifier (DUID). The DUID is carried in client identifier and server identifier options. The DUID is unique across all DHCP clients and servers, and it is stable for any specific client or server. DHCPv6 uses DUIDs based on link-layer addresses for both the client and server identifier. The device uses the MAC address from the lowest-numbered interface to form the DUID. The network interface is assumed to be permanently attached to the device.

When a DHCPv6 client requests two prefixes with the same DUID but with different identity association identifiers (IAIDs) on two different interfaces, these prefixes are considered to be for two different clients, and the interface information is maintained for both.

Rapid Commit

The DHCPv6 client can obtain configuration parameters from a server either through a rapid two-message exchange (solicit, reply) or through a four-message exchange (solicit, advertise, request, and reply). By default, the four-message exchange is used. When the rapid-commit option is enabled by both the client and the server, the two-message exchange is used.

DHCPv6 Client and Relay Functions

The DHCPv6 client and relay functions are mutually exclusive on an interface. When one of these functions is enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: “Interface is in DHCP client mode” or “Interface is in DHCP relay mode.”

The following sections describe these functions:

Client Function

The DHCPv6 client function can be enabled on individual IPv6-enabled interfaces.



Note You need APPX license package to enable the DHCPv6 client function on the device.

The DHCPv6 client can request and accept those configuration parameters that do not require a server to maintain any dynamic state for individual clients, such as DNS server addresses and domain search list options.

The DHCPv6 client can also request the delegation of prefixes. The prefixes acquired from a delegating device will be stored in a local IPv6 general prefix pool. The prefixes in the general prefix pool can then be referred to from other applications; for example, the general prefix pool can be used to number device downstream interfaces.

For IPv6, the details of the default gateway are received from router advertisement (RA) and not from the DHCP server. The details of the default gateway obtained from the DHCP server are not added in the client server. Hence, the following IPv6 commands must be configured on the client interface:

- `pv6 nd autoconfig prefix`
- `“ipv6 nd autoconfig default”`

Server Selection

A DHCPv6 client builds a list of potential servers by sending a solicit message and by collecting advertise message replies from servers. These messages are ranked based on the preference value, and servers may add a preference option to their advertise messages explicitly stating their preference value. If the client needs to acquire prefixes from servers, only servers that have advertised prefixes are considered.

IAPD and IAID

An Identity Association for Prefix Delegation (IAPD) is a collection of prefixes assigned to a requesting device. A requesting device may have more than one IAPD; for example, one for each of its interfaces.

Each IAPD is identified by an IAID. The IAID is chosen by the requesting device and is unique among the IAPD IAIDs on the requesting device. IAIDs are made consistent across reboots by using information from the associated network interface, which is assumed to be permanently attached to the device.

DHCPv6 Relay Agent

A DHCPv6 relay agent, which may reside on the client's link, is used to relay messages between the client and the server. The DHCPv6 relay agent operation is transparent to the client. A DHCPv6 client locates a DHCPv6 server using a reserved, link-scoped multicast address. For direct communication between the DHCPv6 client and the DHCPv6 server, both of them must be attached to the same link. However, in some situations where ease of management, economy, or scalability is a concern, it is desirable to allow a DHCPv6 client to send a message to a DHCPv6 server that is not connected to the same link. IPv6 enable is required for IPv6 DHCP relay, although IPv6 address is configured.

DHCPv6 Relay Agent Notification for Prefix Delegation

The DHCPv6 relay agent notification for prefix delegation allows the device working as a DHCPv6 relay agent to find prefix delegation options by reviewing the contents of a DHCPv6 RELAY-REPLY packet that is relayed by the relay agent to the client. When a prefix delegation option is found by the relay agent, the relay agent extracts the information about the prefix that is being delegated and inserts an IPv6 static route matching the prefix delegation information onto the relay agent. Future packets destined to that prefix via relay will be forwarded based on the information contained in the prefix delegation. The IPv6 static route is then left in the routing table until the prefix delegation lease time expires or the relay agent receives a release packet from the client releasing the prefix delegation.

No user configuration is required for this feature. Static route management is done automatically by the relay agent.

IPv6 routes are added when the relay agent relays a RELAY-REPLY packet, and IPv6 routes are deleted when the prefix delegation lease time expires or the relay agent receives a release message. An IPv6 static route in the routing table of the relay agent can be updated when the prefix delegation lease time is extended.

The DHCP—DHCPv6 Relay Agent Notification for Prefix Delegation feature leaves a static IPv6 route on the routing table of the relay agent. The registered IPv6 address allows unicast reverse packet forwarding (uRPF) to work by allowing the device doing the reverse lookup to confirm that the IPv6 address on the relay agent is not malformed or spoofed. The static route that remains in the routing table of the relay agent can be redistributed to other routing protocols to advertise the subnets to other nodes. Static routes will be removed when a DHCP_DECLINE message is sent by the client.

DHCPv6 Relay Options: Remote-ID for Gigabit Ethernet and Fast Ethernet Interfaces

The DHCPv6 Ethernet Remote ID Option feature adds the remote identification (remote-ID) option to relayed (RELAY-FORWARD) DHCPv6 packets.

The remote-ID option provides information to the DHCPv6 server, which includes port information, the system's DUID, and the VLAN ID. This information can be used to uniquely identify both the relay and the port on the relay through which the client packet arrived. The DHCPv6 server uses this information to select parameters specific to a particular user, host, or subscriber modem.

The addition of the remote-ID option to the RELAY-FORWARD packet occurs automatically and no user configuration is necessary.

The DHCPv6 server does not need to echo the remote-ID option in the RELAY-REPLY packet. The Internet Assigned Numbers Authority (IANA) has assigned the DHCPv6 option code 37 for the relay agent remote-ID option.

If the remote-ID option is included in the RELAY-REPLY packet, the option is removed from the packet before it is relayed to the client.

DHCPv6 Relay Options: Reload Persistent Interface ID

The DHCPv6 Relay—Reload Persistent Interface ID Option feature makes the interface ID option persistent. The interface ID is used by relay agents to decide which interface should be used to forward a RELAY-REPLY packet. A persistent interface-ID option will not change if the device acting as a relay agent goes offline during a reload or a power outage. When the device acting as a relay agent returns online, it is possible that changes to the internal interface index of the relay agent may have occurred in certain scenarios (such as, when the relay agent reboots and the number of interfaces in the interface index changes, or when the relay agents boot up and has more virtual interfaces than it did before the reboot). This feature prevents such scenarios from causing any problems.

This feature changes the DHCPv6 interface-ID option to be expressed as the short form of the interface name. The interface name as the DHCPv6 interface ID helps avoid potential problems that could arise due to physical or logical interfaces changing on the relay agent after a reload.

DHCPv6 Relay Chaining

DHCPv6 messages can be relayed through multiple relay agents. This configuration is called *relay chaining*. A relay chaining configuration can be supported only when each relay agent adds information to DHCPv6 messages before relaying them. The information helps in relaying the DHCPv6 reply back to the DHCPv6 client through the same path.

The delegated IPv6 prefix must be routable in order to be useful. The actual DHCPv6 Prefix Delegation (PD) client may not be permitted to inject routes into the delegating network. In service provider (SP) networks, for example, an edge device typically acts as a DHCPv6 relay agent, and this edge device often has the responsibility to maintain routes within the SP network for clients' PD bindings. In the event that DHCPv6 requests and responses are relayed through a chain of DHCPv6 relays, there may be a need to introduce appropriate routes (particularly with DHCPv6 PD) in the Forwarding Information Base (FIB) so that routing is handled transparently.

DHCPv6 Relay SSO and ISSU

In specific Cisco networking devices that support dual route processors (RPs), stateful switchover (SSO) takes advantage of RP redundancy to increase network availability. The feature establishes one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them.

The Cisco IOS XE In Service Software Upgrade (ISSU) process allows the Cisco IOS XE software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades

are a significant cause of downtime. The ISSU allows the Cisco IOS XE software to be modified while packet forwarding continues. This increases network availability and reduces downtime caused by planned software upgrades.

The SSO and the ISSU use redundant hardware, with the active and standby RP each running an instance of the DHCPv6 relay agent. Both instances exchange run-time state data.

For further information about the SSO and the ISSU, see the “[Stateful Switchover](#)” and the “[Cisco IOS XE In Service Software Upgrade](#)” modules respectively, in the [Cisco IOS High Availability Configuration Guide](#).

DHCPv6 Relay Options: Remote-ID for Ethernet Interfaces

This feature adds the remote identification (remote-ID) option to relayed (RELAY-FORWARD) DHCPv6 packets.

The remote-ID option provides information to the DHCPv6 server, including port information, the system’s DUID, and the VLAN ID. Collectively, this information can be used to uniquely identify both the relay and the port on the relay through which the client’s packet arrived. The DHCPv6 server uses this information to select parameters specific to a particular user, host, or subscriber modem. This feature works only for Ethernet interfaces at this time.

This feature introduces no user configuration. Because the addition of the remote-ID option to the RELAY-FORWARD packet occurs automatically, no user configuration is necessary.

The DHCPv6 server does not need to echo the remote-ID option in the RELAY-REPLY packet. Internet Assigned Numbers Authority (IANA) has assigned the DHCPv6 option code 37 for the relay agent remote-ID option.

If the remote-ID option is included in the RELAY-REPLY packet, the option is stripped out of the packet before the packet is relayed to the client.

DHCPv6 Relay Options: Reload Persistent Interface-ID

This feature makes the interface-ID option, which is used by relay agents to decide which interface should be used when forwarding a RELAY-REPLY packet, persistent. A persistent interface-ID option will not change if the router acting as a relay agent goes offline (such as during a reload or a power outage). When the router acting as a relay agent returns online, it is possible that changes to the internal interface index of the relay agent may have occurred in certain scenarios (such as cases where the relay agent reboots and has a change in the number of interfaces in the interface index, or the relay agents boots up and has more virtual interfaces than it did before the reboot). This feature prevents this scenario from causing any problems.

This feature changes the DHCPv6 interface-ID option to be expressed as simply the short form of the interface name. This syntax helps avoid potential problems that could arise due to physical or logical interfaces changing on the relay agent after a reload.

How to Implement DHCP for IPv6

Configuring the DHCPv6 Server Function

Configuring the DHCPv6 Configuration Pool

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **domain-name** *domain*
5. **dns-server** *ipv6-address*
6. **prefix-delegation** *ipv6-prefix / prefix-length client-duid [iaid iaaid] [lifetime]*
7. **prefix-delegation pool** *poolname [lifetime valid-lifetime preferred-lifetime]*
8. **exit**
9. **interface** *type number*
10. **ipv6 dhcp server** *poolname [rapid-commit] [preference value] [allow-hint]*
11. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ipv6 dhcp pool <i>poolname</i> Example: Device(config)# ipv6 dhcp pool pool1 | Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode. The <i>pool name</i> can be a string, such as "abcd" or an integer value, such as 0. During execution, the configuration mode changes to DHCPv6 pool configuration mode. In this mode, you can configure pool parameters, such as prefixes to be delegated, DNS servers, and so on. |
| Step 4 | domain-name <i>domain</i> Example: Device(config-dhcp)# domain-name example.com | Configures a domain name for a DHCPv6 client. |

| | Command or Action | Purpose |
|---------|--|---|
| Step 5 | <p>dns-server <i>ipv6-address</i></p> <p>Example:</p> <pre>Device(config-dhcp)# dns-server 2001:DB8:3000:3000::42</pre> | Specifies the DNS IPv6 servers available to a DHCPv6 client. |
| Step 6 | <p>prefix-delegation <i>ipv6-prefix / prefix-length client-duid</i> [<i>iaid iaaid</i>] [<i>lifetime</i>]</p> <p>Example:</p> <pre>Device(config-dhcp)# prefix-delegation 2001:DB8:1263::/48 0005000400F1A4D070D03</pre> | Specifies a manually configured numeric prefix to be delegated to a specified client's IAPD. |
| Step 7 | <p>prefix-delegation pool <i>poolname</i> [lifetime <i>valid-lifetime preferred-lifetime</i>]</p> <p>Example:</p> <pre>Device(config-dhcp)# prefix-delegation pool pool1 lifetime 1800 60</pre> | <p>Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCPv6 clients.</p> <p>The lifetime values are <i>valid-lifetime</i> and <i>preferred-lifetime</i>. These are referred to as T1 and T2. When the T2 expires, a renew request is sent to the particular server and if the client does not get a response within T1, the client sends a REBIND request to all available servers.</p> <p>The value of lifetime can be specified as:</p> <ul style="list-style-type: none"> • a fixed duration that remains constant across consecutive advertisements • absolute expiration time in the future, so that the advertised lifetime decrements in real time and is equal to zero at the specified time. <p>The specified duration is between 60 and 4294967295 seconds or infinity if the keyword infinite is specified. If the lifetimes are not specified, by default, the <i>valid-lifetime</i> is 2592000 seconds (or 30 days) and the <i>preferred-lifetime</i> is 604800 seconds (or 7 days).</p> |
| Step 8 | <p>exit</p> <p>Example:</p> <pre>Device(config-dhcp)# exit</pre> | Exits DHCPv6 pool configuration mode, and returns the device to global configuration mode. |
| Step 9 | <p>interface <i>type number</i></p> <p>Example:</p> <pre>Device(config)# interface serial 3</pre> | Specifies an interface type and number, and enters interface configuration mode. |
| Step 10 | <p>ipv6 dhcp server <i>poolname</i> [rapid-commit] [preference <i>value</i>] [allow-hint]</p> | Enables or disables DHCPv6 service on an interface. |

| | Command or Action | Purpose |
|----------------|---|---|
| | <p>Example:</p> <pre>Device(config-if)# ipv6 dhcp server pool1</pre> | <ul style="list-style-type: none"> If specified, rapid-commit enables the use of the two-message exchange for prefix delegation and other configuration. If the rapid-commit option is used in the Solicit message and rapid-commit is enabled for the server, the server responds to the Solicit with a Reply message. By default, rapid-commit is disabled. Default value of preference is 0. If the allow-hint option is specified, is a valid prefix in the associated local prefix pool and is not assigned to anybody, the server delegates the client-suggested prefix in the Solicit and Request messages. Otherwise, the hint is ignored and a prefix is delegated from the free list in the pool. <p>Note By default, DHCPv6 service on an interface is disabled.</p> |
| Step 11 | <p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre> | Returns to privileged EXEC mode. |

Configuring a Binding Database Agent for the Server Function

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp database agent [write-delay seconds] [timeout seconds]**
4. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | <p>enable</p> <p>Example:</p> <pre>Device> enable</pre> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | <p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | <p>ipv6 dhcp database agent [write-delay seconds] [timeout seconds]</p> | Specifies DHCPv6 binding database agent parameters. |

| | Command or Action | Purpose |
|---------------|---|---|
| | <p>Example:</p> <pre>Device(config)# ipv6 dhcp database tftp://10.0.0.1/dhcp-binding</pre> | <ul style="list-style-type: none"> • agent-URL—flash, NVRAM, FTP, TFTP, or RCP uniform resource locator. • write-delay—specifies how often DHCP sends database updates. By default, DHCPv6 server waits 300 seconds before transmitting database changes. The minimum delay is 60 seconds. • timeout—specifies the time to wait for a database transfer. Infinity is defined as zero seconds. Transfers that exceed the timeout period are aborted. Default value is 300 seconds. |
| Step 4 | <p>end</p> <p>Example:</p> <pre>Device(config)# end</pre> | Returns to privileged EXEC mode. |

Configuring the DHCPv6 Client Function

General prefixes can be defined dynamically from a prefix received by a DHCPv6 prefix delegation client. The delegated prefix is stored in a general prefix.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 dhcp client pd** {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**]
5. **ipv6 nd autoconfig prefix**
6. **ipv6 nd autoconfig default-router**
7. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | <p>enable</p> <p>Example:</p> <pre>Device> enable</pre> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | <p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre> | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 3 | interface <i>type number</i> Example: Device(config)# interface fastethernet 0/0/0 | Specifies an interface type and number, and enters interface configuration mode. |
| Step 4 | ipv6 dhcp client pd { <i>prefix-name</i> hint <i>ipv6-prefix</i> } [rapid-commit] Example: Device(config-if)# ipv6 dhcp client pd dhcp-prefix | Enables the DHCPv6 client process and enables a request for prefix delegation through a specified interface. Note The ipv6 dhcp client pd hint command should always be used along with the ipv6 dhcp client pd <i>pd-name</i> command. |
| Step 5 | ipv6 nd autoconfig prefix Example: Device(config-if)# ipv6 nd autoconfig prefix | Allows Neighbor Discovery to install all valid on-link prefixes from router advertisements (RAs) received on the interface. |
| Step 6 | ipv6 nd autoconfig default-router Example: Device(config-if)# ipv6 nd autoconfig default-router | Allows Neighbor Discovery to install a default route to the Neighbor Discovery-derived default router. |
| Step 7 | end Example: Device(config-if)# end | Returns to privileged EXEC mode. |

Example

The following example depicts the usage of **ipv6 dhcp client pd hint** command along with the **ipv6 dhcp client pd *pd-name*** command.

```
interface GigabitEthernet0/10
no ip address
media-type auto-select
negotiation auto
ipv6 address prefix-from-provider ::1/48
ipv6 enable
ipv6 dhcp client pd hint 2001:DB8:43::/48
ipv6 dhcp client pd prefix-from-provider
```

Configuring the DHCPv6 Relay Agent

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*

4. **ipv6 enable**
5. **ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number*]
6. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | interface <i>type number</i> Example: <pre>Device(config)# interface gigabitethernet 4/2/0</pre> | Specifies an interface type and number, and enters interface configuration mode. |
| Step 4 | ipv6 enable Example: <pre>Device(config-if)# ipv6 enable</pre> | Enables IPv6 processing on an interface. |
| Step 5 | ipv6 dhcp relay destination <i>ipv6-address</i> [<i>interface-type interface-number</i>] Example: <pre>Device(config-if) ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 gigabitethernet 4/3/0</pre> | Specifies a destination address to which client packets are forwarded and enables the DHCPv6 relay service on the interface. |
| Step 6 | end Example: <pre>Device(config-if)# end</pre> | Returns to privileged EXEC mode. |

Configuring Route Addition for Relay and Server

To enable route addition by DHCPv6 relay and server for the delegated prefix, use the **ipv6 dhcp iapd-route-add** command in global configuration mode.

DHCPv6 relay inserts a route for the delegated prefix without additional configuration (i.e., the default is **ipv6 dhcp iapd-route-add**, which of course isn't NVGEN'ed.) If you want to disable this insertion, you must configure **no ipv6 dhcp iapd-route-add**.

The relay tracks valid and preferred lifetimes for the delegated prefix. When the prefix reaches the end of the valid lifetime, the route is automatically removed from the routing table.

To add routes for individually assigned IPv6 addresses on the relay or server, use the **ipv6 dhcp iana-route-add** command in global configuration mode.

Defining a General Prefix with the DHCPv6 Prefix Delegation Client Function

Perform this task to configure the DHCPv6 client function on an interface and enable prefix delegation on an interface. The delegated prefix is stored in a general prefix.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 dhcp client pd** {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**]

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | interface <i>type number</i> Example: Device(config)# interface gigabitethernet 0/0/0 | Specifies an interface type and number, and enters interface configuration mode. |
| Step 4 | ipv6 dhcp client pd { <i>prefix-name</i> hint <i>ipv6-prefix</i> } [rapid-commit] Example: Device(config-if)# ipv6 dhcp client pd dhcp-prefix | Enables the DHCPv6 client process and enables a request for prefix delegation through a specified interface. <ul style="list-style-type: none">• The delegated prefix is stored in the general prefix <i>prefix-name</i> argument. |

Configuring a VRF-Aware Relay for MPLS VPN Support

Configuring a VRF-Aware Relay



Note You do not have to configure this feature on specified interfaces. If you want the feature to be enabled globally only on a device, perform steps 1, 2, and 3

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp-relay option vpn**
4. **interface** *type number*
5. **ipv6 dhcp relay option vpn**
6. **ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number* | **vrf** *vrf-name* | **global**]
7. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ipv6 dhcp-relay option vpn Example: Device(config)# ipv6 dhcp-relay option vpn | Enables the DHCP for IPv6 relay VRF-aware feature globally. |
| Step 4 | interface <i>type number</i> Example: Device(config)# interface gigabitethernet 0/0/0 | Specifies an interface type and number, and enters interface configuration mode. |
| Step 5 | ipv6 dhcp relay option vpn Example: Device(config-if)# ipv6 dhcp relay option vpn | Enables the DHCP for IPv6 relay VRF-aware feature on the specified interface. Enabling this command supersedes the configuration that is enabled by using the ipv6 dhcp-relay option vpn command. |
| Step 6 | ipv6 dhcp relay destination <i>ipv6-address</i> [<i>interface-type interface-number</i> vrf <i>vrf-name</i> global] Example: Device(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 ethernet 0/0 | Specifies a destination address to which client messages are forwarded. |
| Step 7 | end Example: Device(config-if)# end | Returns to privileged EXEC mode. |

Restarting the DHCPv6 Client on an Interface

Perform this task to restart the DHCPv6 client on a specified interface after first releasing and unconfiguring previously acquired prefixes and other configuration options.

SUMMARY STEPS

1. **enable**
2. **clear ipv6 dhcp client** *interface-type interface-number*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | clear ipv6 dhcp client <i>interface-type interface-number</i> Example: Device# clear ipv6 dhcp client GigabitEthernet 1/0/0 | Restarts the DHCPv6 client on an interface. |

Deleting Automatic Client Bindings from the DHCPv6 Binding Table

SUMMARY STEPS

1. **enable**
2. **clear ipv6 dhcp binding** [*ipv6-address*] [**vrf** *vrf-name*]

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | clear ipv6 dhcp binding [<i>ipv6-address</i>] [vrf <i>vrf-name</i>] Example: Device# clear ipv6 dhcp binding | Deletes automatic client bindings from the DHCPv6 binding table. |

Troubleshooting DHCPv6



Note Step 1 is common to each debug command. Step 2 to Step 5 are separate debugging commands that can be used in any order.

SUMMARY STEPS

1. `enable`
2. `debug ipv6 dhcp [detail]`
3. `debug ipv6 dhcp database`
4. `debug ipv6 dhcp relay`
5. `debug ipv6 dhcp redundancy [detail]`

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | debug ipv6 dhcp [detail] Example: Device# debug ipv6 dhcp | Enables debugging for DHCPv6. |
| Step 3 | debug ipv6 dhcp database Example: Device# debug ipv6 dhcp database | Enables debugging for the DHCPv6 binding database. |
| Step 4 | debug ipv6 dhcp relay Example: Device# debug ipv6 dhcp relay | Enables DHCPv6 relay agent debugging. |
| Step 5 | debug ipv6 dhcp redundancy [detail] Example: Device# debug ipv6 dhcp redundancy | Enables DHCPv6 redundancy debugging. |

Verifying the DHCPv6 Configuration

SUMMARY STEPS

1. `enable`
2. `show ipv6 dhcp`
3. `show ipv6 dhcp binding [ipv6-address]`

4. **show ipv6 dhcp database** [*agent-URL*]
5. **show ipv6 dhcp interface** [*type number*]
6. **show ipv6 dhcp pool** [*poolname*]
7. **show running-config**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device# enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | show ipv6 dhcp Example: Device# show ipv6 dhcp | Displays the DUID on a specified device. |
| Step 3 | show ipv6 dhcp binding [<i>ipv6-address</i>] Example: Device# show ipv6 dhcp binding | Displays automatic client bindings from the DHCPv6 database. |
| Step 4 | show ipv6 dhcp database [<i>agent-URL</i>] Example: Device# show ipv6 dhcp database | Displays the DHCPv6 binding database agent information. |
| Step 5 | show ipv6 dhcp interface [<i>type number</i>] Example: Device# show ipv6 dhcp interface | Displays DHCPv6 interface information. |
| Step 6 | show ipv6 dhcp pool [<i>poolname</i>] Example: Device# show ipv6 dhcp pool | Displays DHCPv6 configuration pool information. |
| Step 7 | show running-config Example: Device# show running-config | Displays the current configuration running on the router. |

Example Verifying the DHCPv6 Configuration

Sample Output from the show ipv6 dhcp Command

The following sample output from the **show ipv6 dhcp** command displays the DUID of the device:

```
Device# show ipv6 dhcp
```

```
This device's DHCPv6 unique identifier(DUID): 000300010002FCA5DC1C
```


Sample Output from the show ipv6 dhcp binding Command

In the following sample output, the **show ipv6 dhcp binding** command displays information about two clients, including their DUIDs, IAPDs, prefixes, and preferred and valid lifetimes:

```
Device# show ipv6 dhcp binding

Client: FE80::202:FCFF:FEA5:DC39 (GigabitEthernet2/1/0)
DUID: 000300010002FCA5DC1C
IA PD: IA ID 0x00040001, T1 0, T2 0
Prefix: 3FFE:C00:C18:11::/68
preferred lifetime 180, valid lifetime 12345
expires at Nov 08 2002 02:24 PM (12320 seconds)
Client: FE80::202:FCFF:FEA5:C039 (GigabitEthernet2/1/0)
DUID: 000300010002FCA5C01C
IA PD: IA ID 0x00040001, T1 0, T2 0
Prefix: 3FFE:C00:C18:1::/72
preferred lifetime 240, valid lifetime 54321
expires at Nov 09 2002 02:02 AM (54246 seconds)
Prefix: 3FFE:C00:C18:2::/72
preferred lifetime 300, valid lifetime 54333
expires at Nov 09 2002 02:03 AM (54258 seconds)
Prefix: 3FFE:C00:C18:3::/72
preferred lifetime 280, valid lifetime 51111
```

Sample Output from the show ipv6 dhcp database Command

The following sample output from the **show ipv6 dhcp database** command shows information on the binding database agents TFTP, NVRAM, and flash:

```
Device# show ipv6 dhcp database

Database agent tftp://172.19.216.133/db.tftp:
write delay: 69 seconds, transfer timeout: 300 seconds
last written at Jan 09 2003 01:54 PM,
write timer expires in 56 seconds
last read at Jan 06 2003 05:41 PM
successful read times 1
failed read times 0
successful write times 3172
failed write times 2
Database agent nvram:/dhcpv6-binding:
write delay: 60 seconds, transfer timeout: 300 seconds
last written at Jan 09 2003 01:54 PM,
write timer expires in 37 seconds
last read at never
successful read times 0
failed read times 0
successful write times 3325
failed write times 0
Database agent flash:/dhcpv6-db:
write delay: 82 seconds, transfer timeout: 3 seconds
last written at Jan 09 2003 01:54 PM,
write timer expires in 50 seconds
last read at never
successful read times 0
failed read times 0
successful write times 2220
failed write times 614
```

Sample Output from the show ipv6 dhcp interface Command

The following is sample output from the **show ipv6 dhcp interface** command. In the first example, the command is used on a device that has an interface acting as a DHCPv6 server. In the second example, the command is used on a router that has an interface acting as a DHCPv6 client:

```
Device# show ipv6 dhcp interface

GigabitEthernet2/1/0 is in server mode
Using pool: svr-p1
Preference value: 20
Rapid-Commit is disabled
Router2# show ipv6 dhcp interface
GigabitEthernet2/1/0 is in client mode
State is OPEN (1)
List of known servers:
Address: FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
Preference: 20
IA PD: IA ID 0x00040001, T1 120, T2 192
Prefix: 3FFE:C00:C18:1::/72
preferred lifetime 240, valid lifetime 54321
expires at Nov 08 2002 09:10 AM (54319 seconds)
Prefix: 3FFE:C00:C18:2::/72
preferred lifetime 300, valid lifetime 54333
expires at Nov 08 2002 09:11 AM (54331 seconds)
Prefix: 3FFE:C00:C18:3::/72
preferred lifetime 280, valid lifetime 51111
expires at Nov 08 2002 08:17 AM (51109 seconds)
DNS server: 2001:DB8:1001::1
DNS server: 2001:DB8:1001::2
Domain name: example1.net
Domain name: example2.net
Domain name: example3.net
Prefix name is cli-pl
Rapid-Commit is enabled
```

Sample Output from the show ipv6 dhcp pool Command

In the following sample output, the **show ipv6 dhcp pool** command displays information about the configuration pool named svr-p1, including static bindings, prefix information, the DNS server, and the domain names found in the svr-p1 pool:

```
Device# show ipv6 dhcp pool

DHCPv6 pool: svr-p1
Static bindings:
Binding for client 000300010002FCA5C01C
IA PD: IA ID 00040002,
Prefix: 3FFE:C00:C18:3::/72
preferred lifetime 604800, valid lifetime 2592000
IA PD: IA ID not specified; being used by 00040001
Prefix: 3FFE:C00:C18:1::/72
preferred lifetime 240, valid lifetime 54321
Prefix: 3FFE:C00:C18:2::/72
preferred lifetime 300, valid lifetime 54333
Prefix: 3FFE:C00:C18:3::/72
preferred lifetime 280, valid lifetime 51111
Prefix from pool: local-pl, Valid lifetime 12345, Preferred lifetime 180
DNS server: 2001:DB8:1001::1
DNS server: 2001:DB8:1001::2
Domain name: example1.net
Domain name: example2.net
Domain name: example3.net
```

```

Active clients: 2
Current configuration : 22324 bytes
!
! Last configuration change at 14:59:38 PST Tue Jan 16 2009
! NVRAM config last updated at 04:25:39 PST Tue Jan 16 2009 by name01
!
hostname Router
!
ip cef
ipv6 unicast-routing
ipv6 cef
ipv6 cef accounting prefix-length
!
!
interface GigabitEthernet0/0/0
ip address 10.4.9.11 255.0.0.0
media-type 10BaseT
ipv6 address 2001:DB8:C18:1::/64 eui-64

```

Configuration Examples for Implementing DHCPv6

Example: Configuring the DHCPv6 Client Function

In the following example, this Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client has three interfaces. Ethernet interface 0/0 is the upstream link to a service provider, which has a DHCPv6 server function enabled. The Fast Ethernet interfaces 0/0 and 0/1 are links to local networks.

The upstream interface, Ethernet interface 0/0, has the DHCPv6 client function enabled. Prefixes delegated by the provider are stored in the general prefix called prefix-from-provider.

The local networks, Fast Ethernet interfaces 0/0 and 0/1, both assign interface addresses based on the general prefix called prefix-from-provider. The bits on the left of the addresses come from the general prefix, and the bits on the right of the addresses are specified statically.

```

interface Ethernet 0/0
description uplink to provider DHCP IPv6 server
ipv6 dhcp client pd prefix-from-provider
!
interface FastEthernet 0/0
description local network 0
ipv6 address prefix-from-provider ::5:0:0:0:100/64
!
interface FastEthernet 0/1
description local network 1
ipv6 address prefix-from-provider ::6:0:0:0:100/64

```

